BY ORDER OF THE COMMANDER,
PACIFIC AIR FORCES

AIR FORCE SYSTEMS SECURITY
INSTRUCTION 5021

PACIFIC AIR FORCES COMMAND
Supplement 1

25 JULY 2003

Communications and Information

TIME COMPLIANCE NETWORK ORDER (TCNO) MANAGEMENT AND VULNERABILITY AND INCIDENT REPORTING

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

NOTICE: This publication is available digitally on the AFDPO WWW site at: **http://www.e-publishing.af.mil.**

OPR: HQ PACAF/SCI (TSgt John F. Daniels)

Certified by: HQ PACAF/SCI
(Lt Col Victor J. Diaz)

Supersedes AFSSI5021_PACAFSUP1,
12 February 2003 and IC 2003-1,
25 July 2003

Pages: 9
Distribution: F

This supplement applies to all personnel that use, administer or manage automated information systems, business-applications, or computer networks in PACAF. It does not apply to the Air National Guard (ANG) or the Air Force Reserve Command (AFRC) units.

SUMMARY OF REVISIONS

This change incorporates interim change (IC) 2003-1 (**Attachment 14 (Added)**) which adds procedures and CONOPS to the PACAF wireless network scanning initiative. This change sets forth operating and reporting procedures for wireless networks and devices found on the PACAF Enterprise. A bar (|) indicates revision from previous edition.

AFSSI 5021, 1 March 2001, is supplemented as follows:

3.1. **General.** These are the minimum required policies, procedures, and report formats to handle, process, and report Internet Security Systems (ISS) Network Scanning and Vulnerability Reporting. Internet Scanner is the Air Force's network scanning tool of choice and is part of the Combat Information Transport System/Base Information Protect initiative. Additionally, this section will cover reporting unauthorized network activity and security incidents. Incidents include vulnerabilities, classified message incidents (CMIs), and intrusions. This policy is based on near real-time detection, containment, recovery, and mission-impact/damage-assessment reporting.

3.1.1. (Added) Internet Security Systems. ISS Internet Scanner is the Air Force's network scanning tool of choice and is fielded at all Air Force bases as part of the approved Combat Information Transport System/Network Management System /Base Information Protect (CITS NMS/BIP) toolset. As such, all PACAF bases must use Internet Scanner to perform network vulnerability scans. Each base will ensure that at least one individual is Internet Scanner certified at all times in order to receive the ISS key, which are ordered approximately every six months. This "certified" individual can train others in the crew position but he/she cannot certify them. To obtain certification status individuals must attend formal Air Force training. Only certified individuals are authorized to order keys to enable the scanner to work on the bases' IP ranges. Under no circumstances will an individual who has not been trained to use this intrusive tool perform any scans. Maintaining qualified individuals is the responsibility of the Communication Squadron Commanders. Report immediately to the PACAF Network Operations Center (NOSC) if you do not have a certified individual.

3.1.2. (Added) . Internet Security Systems Wireless Scanner is PACAF's wireless network scanning tool of choice and is fielded to all PACAF bases as an enhancement to the approved CITS NMS/BIP toolset. As such, all PACAF bases must use Wireless Scanner to perform wireless network vulnerability scans. Each base has at least one individual who is Internet Scanner certified. His/her duties will encompass ISS Wireless Scanner. This Internet Scanner "certified" individual can train others in the crew position but he/she cannot certify them.

3.1.2.1. (Added) Ministumbler is a used to pinpoint wireless networks while walking through buildings. It will not test for vulnerabilities but will aid in the location of wireless devices on PACAF installations.

3.5.1.1. (Added) Two types of scans will be conducted. Each base will conduct internal (inside the firewall) scans and the NOSC will conduct external scans (DMZ). Coordination between the Air Force Communications Emergency Response Team (AFCERT), NOSC, NCC, and any affected users is mandatory and must be clearly documented prior to any scan or rescan. It is recommended that individual workstations be scanned at night to avoid crashes and network traffic delays.

3.5.1.2. (Added) The Wing Information Assurance Office (WIAO) working in conjunction with the NCC (Information System Security Manager (ISSM)) and Wing/Unit COMPUSEC (Information System Security Officer (ISSO)) managers will track and report fix actions on vulnerabilities discovered during both internal and external scans to the PACAF NOSC. Further coordination with the Wing/Squadron COMPUSEC manager might be required for resolution. Fix actions may include applying corrective measures (i.e. patches and configuration changes) in accordance with the timelines established by this policy to eliminate vulnerabilities. Formal MAJCOM Designated Approval Authority (DAA) acceptance of the risk posed by a vulnerability must be documented in the base backbone System Security Authorization Agreement (SSAA) package. Formal Wing Network DAA acceptance of any acceptable risk posed by a vulnerability must be documented in the base unique system SSAA.

3.5.1.3. (Added) All new, rebuilt, or updated (which includes patched, new driver installation, or added hardware) automated information systems must be scanned using ISS as soon as they are connected to the network in accordance with (IAW) PACAF Sup 1 to AFI 33-202, Computer Security. Failure to accomplish this task opens undue risk onto the network and could result in malicious activity. Retain all applicable documentation (ISS scan results, responses from network/system administrators, reports to NOSC, etc) until systems are no longer in use (reference AFMAN 37-139, Table 33-25, Rules 9 and 10). By retaining prior scans, a clear history can be established from the date the system was initially scanned. Additionally, this historical data might assist investigators if a particular system is compromised.

3.5.1.4. (Added) Internal Scans. Each base will conduct internal scans monthly on Non-Secure Internet Protocol Router Network (NIPRNET) and Secret Internet Protocol Router Network (SIPRNET) networks for all critical equipment (listed below) IAW NOSC Communications Tasking Order (CTO) and semi-annually on all workstations. It is vital that directions from the NOSC are strictly adhered to. Scans must be consistent in order to obtain an accurate baseline for further reporting (i.e. same nodes must be identified on re-scans). If your base is tasked to scan 15 IP addresses then the scanning operator and workgroup manager must make sure the target IPs are available to complete the scan. Failure to scan properly only delays the reporting process. PACAF/SCI will provide MAJCOM reporting status as directed by the PACAF/SC. Each base will maintain architectural diagram(s) with machine names and IP(s), and a ports and protocols matrix supporting each configuration for the critical infrastructure. These diagrams and information are necessary to support system analysis. The following is provided to clearly define Critical infrastructure:

3.5.1.4.1. (Added) External router, switches, and any routers occupying the DMZ down to the Premise outer

3.5.1.4.2. (Added) Firewall, all RAS (remote access servers), and ERAS (enhanced remote access server)

3.5.1.4.3. (Added) DNS Server, Proxy Server, Public Web servers, and all intranet web servers

3.5.1.4.4. (Added) PACAF specific systems (i.e. SMTP gateway)

3.5.1.4.5. (Added) All switches, routers, and hubs down to the communication closet

3.5.1.4.6. (Added) All Network Control Center (NCC) server farms to include: Primary Domain Controller, Backup Domain Controllers, Exchange servers, File servers, Bridgehead servers, Remedy servers, and Network Management servers (i.e. ITA & ESM servers, HP Openview, NetIQ).

3.5.1.5. (Added) Complete the initial monthly AIS scans by the fifth duty day of every month. Scan all critical systems connected to the base network using only the NOSC-provided Internet Scanner custom-policy “templates” as appropriate to the specific system (UNIX, NT, CISCO, etc.) located at **https://nosc.pacaf.af.mil**. Without PACAF/SCI approval, no other scan policies should be used to scan PACAF networks. Do not use default policies (i.e. L1 inventory, L2*, L3*, L4*, or L5*) to scan PACAF networks. These policies are not approved and could cause severe damage such as a Denial of Service (DOS) outage. If a scan is conducted and reported to the PACAF NOSC using one of these default policies, the ISS scan operator will be de-certified.

Category	Re-scan due to NOSC	Required Fix Action Date
High	8 calendar days	Patched/fixed in 7 calendar days
Medium	15 calendar days	Patched/fixed in 14 calendar days
Low	Initial monthly scan	Patched/fixed in 30 calendar days

3.5.1.6. (Added) Complete semi-annual workstation scans by 01 Jan and 01 Jul. Scan all workstations connected to the base network using the NOSC-provided ISS custom policies as appropriate to the specific system (UNIX, NT, CISCO, etc.). Do not use default policies (i.e. L1 inventory, L2*, L3*, L4*, or L5*) to scan PACAF workstations. These policies are not approved and could cause severe damage such as a Denial of Service (DOS) outage. With PACAF/SCI concurrence, bases should actively enhance policies for use on their installations by adding additional checks. However, do not change baseline policies without HQ PACAF/SCI approval.

Category	Re-scan due to NOSC	Required Fix Action Date
High	61 calendar days	Patched/fixed in 60 calendar days
Medium	121 calendar days	Patched/fixed in 120 calendar days
Low	semi-annual rescan	Patched/fixed in 150 calendar days

3.5.1.7. (Added) The NOSC will complete external scans on or about the fifth duty day of every month. *If operational requirements prohibit the scan from being accomplished, they will be performed at the first opportunity*. If operational requirements exist they must be documented and submitted to PACAF/SC. These scans will use the appropriate custom policies provided by PACAF/SCI. The NOSC will pre-coordinate all such scans with the NCC. The WIAO and NCCs can request an external scan of a system outside the base firewall at any time by contacting the PACAF NOSC Commander. NOSC, WIAO**,** and NCCs are instructed to close vulnerabilities IAW paragraph **3.5.1.2. (Added)** above.

Category	Re-scan performed by NOSC	Required Fix Action Date
High	30 calendar days	Patched/fixed in 7 calendar days
Medium	"	Patched/fixed in 14 calendar days
Lo	"	Patched/fixed in 30 calendar days

3.5.1.8. (Added) Monthly scans do not need to be published in the CTO in order for a base to complete the required internal scans. The NOSC will maintain the number of High, Medium, and Low vulnerabilities for each base via the NOSC SIPRNET web site. It is the base's responsibility to check this site to verify required rescans and due dates. It is the sole responsibility of each base NCC to ensure scans are conducted and risks mitigated in the timeframes provided. If a base is unable to abide by the timeframes provided, a waiver request must be forwarded to the PACAF NOSC clearly stating the reason for the delay. The PACAF NOSC will forward the request to PACAF/SC for approval. Failure to complete these steps will result in notification to the PACAF/CC.

3.5.1.9. (Added) The WIAO and NCC will report all exceptions and accepted risks they wish to list in the backbone SSAA package to the NOSC for review. The NOSC in association with PACAF/SCI are the sole authorities to determine if an identified vulnerability is in fact a “false positive”. Only after determinations by PACAF/SCI and the NOSC, will these exceptions be accepted and not be held accountable to the base for the vulnerability in future scans. Only after final approval by the PACAF NOSC, may a site add the vulnerabilities to the SSAA IAW PACAF Supp 1 to AFI 33-202 for MAJCOM DAA approval.

3.5.1.10. (Added) It is recommended that the NCC at each installation maintain a Service Level Agreement (SLA) with each Functional System Administrator (FSA) or Work Group Manager (WM) to formalize pre-scan coordination between the NCC and affected users. This MOA will outline responsibilities, procedures, and timelines for correcting any vulnerability detected during a scan.

3.5.1.11. (Added) Forward a copy of the Executive Overview Report (**Attachment 11 (Added)**), the Line Management Report (**Attachment 12 (Added)**), and the Technician report (**Attachment 13 (Added)**) to the SIPRNET NOSC account. Difficulties encountered that prevent compliance within prescribed timelines must be documented IAW paragraph **3.5.1.9. (Added)** above. Naming conventions for NCCs are to be followed IAW C4 NOTAM PACAF 2002-243-004a, Subject; Monthly Internal NIPRNET ISS Scan, para. 5. Monthly scans should be saved as: basename_type_yyyymmdd.rtf. Rescan file names should be saved as: basename_type_yyyymmdd_rescan.rtf. The "type" is either: Int_RS_Exe, Int_RS_Line, Int_RS_Tech. Int_Unix_Exe, Int_Unix_Line, Int_Unix_Tech, Int_Win32_Exe, Int_Win32_Line, or Int_Win32_Tech. Example: Osan_Int_Unix_Line_20021005.rtf and Osan_Int_Unix_Line_20021012_rescan.rtf. Naming conventions for the NOSC will include the Network Defender's name performing the external scan(s). Example basename_type_yyyymmdd_NetworkDefenderName.rtf (_rescan.rtf, if applicable.)

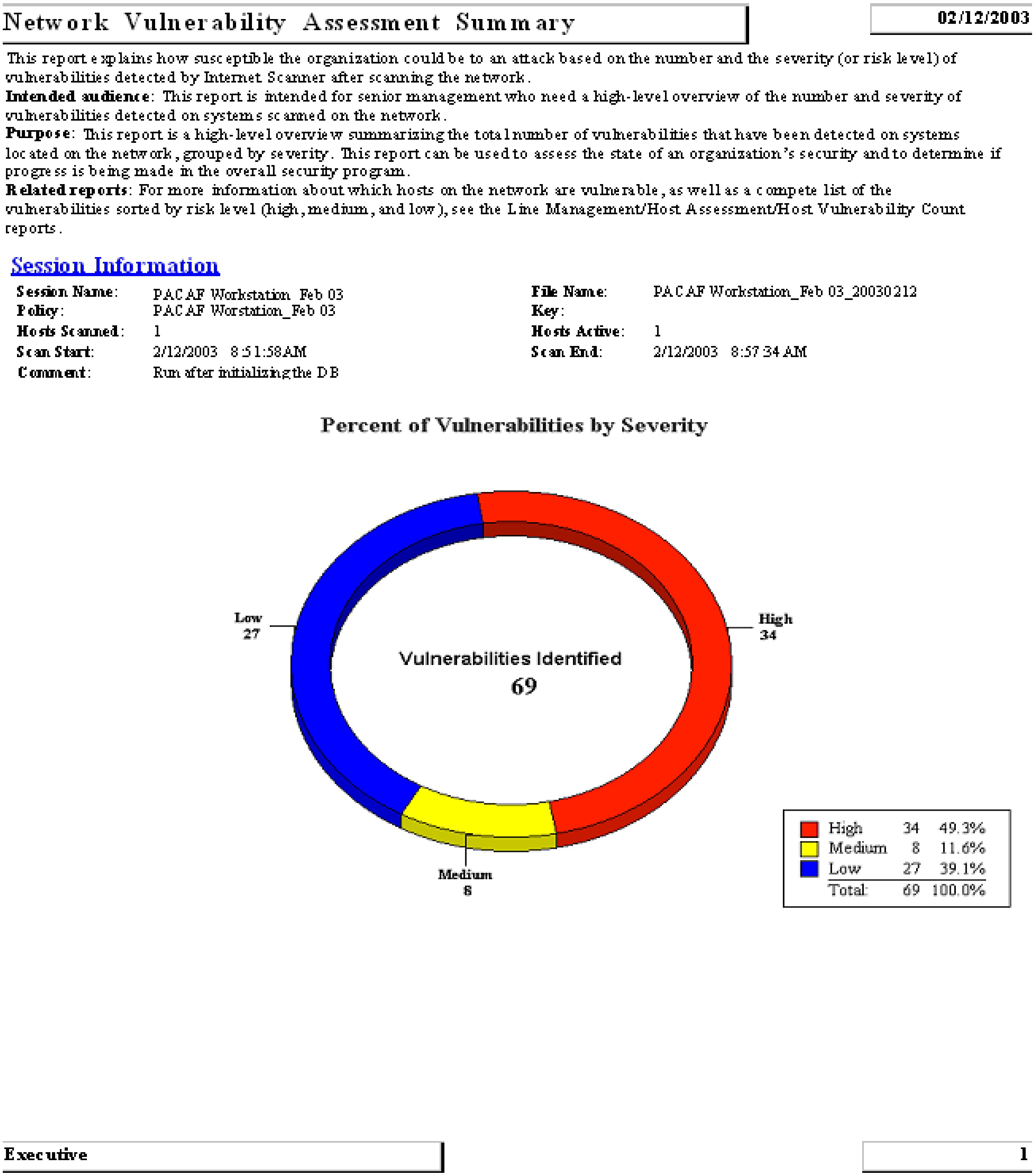
3.5.1.12. (Added) The WIAO and NCC will make every attempt, including elevating through their chain-of-command, to determine if system administrators have taken or will take corrective action. If unable to resolve, include the name of the system involved, contact information, and open work orders. On work orders, include work order number, with who established, contact names/numbers, and an estimated completion date (ECD) in the message body. The Command IA Office will use this information to help resolve as necessary. The WIAO, NCC, and COMPUSEC manager will continue to track status until the vulnerability is closed.

3.5.1.13. (Added) Wireless Scans. Each base will conduct wireless network scans on a periodic basis. This scan will be tasked by a Time Compliance Technical Order (TCTO) on a periodic basis. Upon discovery of a wireless network the ISS technician needs to verify its validity. This is done by verifying a signed AF Form 3215, and a Certificate to Operate from the DAA.

3.5.1.13.1. (Added) If a wireless network is found and is not authorized, a solution for the customer must be presented before any equipment is confiscated.

Attachment 11 (Added)

EXAMPLE EXECUTIVE VULNERABILITY ASSESSMENT REPORT



Network Vulnerability Assessment Summary

02/12/2003

This report explains how susceptible the organization could be to an attack based on the number and the severity (or risk level) of vulnerabilities detected by Internet Scanner after scanning the network.

Intended audience: This report is intended for senior management who need a high-level overview of the number and severity of vulnerabilities detected on systems scanned on the network.

Purpose: This report is a high-level overview summarizing the total number of vulnerabilities that have been detected on systems located on the network, grouped by severity. This report can be used to assess the state of an organization's security and to determine if progress is being made in the overall security program.

Related reports: For more information about which hosts on the network are vulnerable, as well as a compete list of the vulnerabilities sorted by risk level (high, medium, and low), see the Line Management/Host Assessment/Host Vulnerability Count reports.

Session Information

Session Name:	PACAF Workstation_Feb 03	**File Name**:	PACAF Workstation_Feb 03_20030212
Policy:	PACAF Worstation_Feb 03	**Key**:	
Hosts Scanned:	1	**Hosts Active**:	1
Scan Start:	2/12/2003 8:51:58AM	**Scan End**:	2/12/2003 8:57 34 AM
Comment:	Run after initializing the DB		

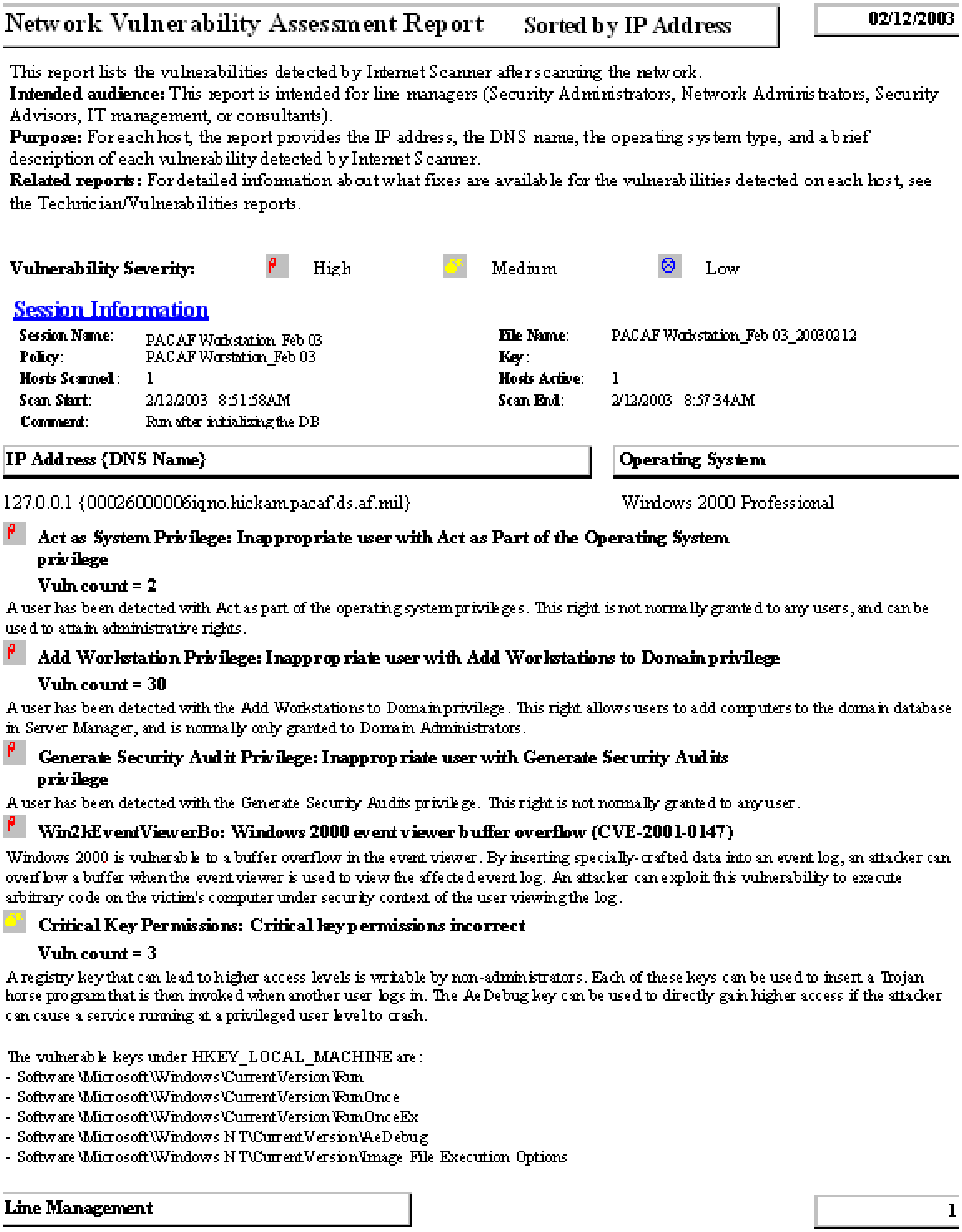
Percent of Vulnerabilities by Severity

🟥	High	34	49.3%
🟨	Medium	8	11.6%
🟦	Low	27	39.1%
	Total:	69	100.0%

Executive 1

Attachment 12 (Added)

EXAMPLE LINE MANAGEMENT VULNERABILITY ASSESSMENT REPORT



Network Vulnerability Assessment Report Sorted by IP Address | 02/12/2003

This report lists the vulnerabilities detected by Internet Scanner after scanning the network.
Intended audience: This report is intended for line managers (Security Administrators, Network Administrators, Security Advisors, IT management, or consultants).
Purpose: For each host, the report provides the IP address, the DNS name, the operating system type, and a brief description of each vulnerability detected by Internet Scanner.
Related reports: For detailed information about what fixes are available for the vulnerabilities detected on each host, see the Technician/Vulnerabilities reports.

Vulnerability Severity: 🟥 High 🟨 Medium 🔵 Low

Session Information

Session Name:	PACAF Workstation Feb 03	**File Name:**	PACAF Workstation_Feb 03_20030212
Policy:	PACAF Worstation_Feb 03	**Key :**	
Hosts Scanned :	1	**Hosts Active:**	1
Scan Start:	2/12/2003 8:51:58AM	**Scan End:**	2/12/2003 8:57:34AM
Comment:	Run after initializing the DB		

IP Address {DNS Name}	Operating System
127.0.0.1 {00026000006iqno.hickam.pacaf.ds.af.mil}	Windows 2000 Professional

🟥 **Act as System Privilege: Inappropriate user with Act as Part of the Operating System privilege**

Vuln count = 2

A user has been detected with Act as part of the operating system privileges. This right is not normally granted to any users, and can be used to attain administrative rights.

🟥 **Add Workstation Privilege: Inappropriate user with Add Workstations to Domain privilege**

Vuln count = 30

A user has been detected with the Add Workstations to Domain privilege. This right allows users to add computers to the domain database in Server Manager, and is normally only granted to Domain Administrators.

🟥 **Generate Security Audit Privilege: Inappropriate user with Generate Security Audits privilege**

A user has been detected with the Generate Security Audits privilege. This right is not normally granted to any user.

🟥 **Win2kEventViewerBo: Windows 2000 event viewer buffer overflow (CVE-2001-0147)**

Windows 2000 is vulnerable to a buffer overflow in the event viewer. By inserting specially-crafted data into an event log, an attacker can overflow a buffer when the event viewer is used to view the affected event log. An attacker can exploit this vulnerability to execute arbitrary code on the victim's computer under security context of the user viewing the log.

🟨 **Critical Key Permissions: Critical key permissions incorrect**

Vuln count = 3

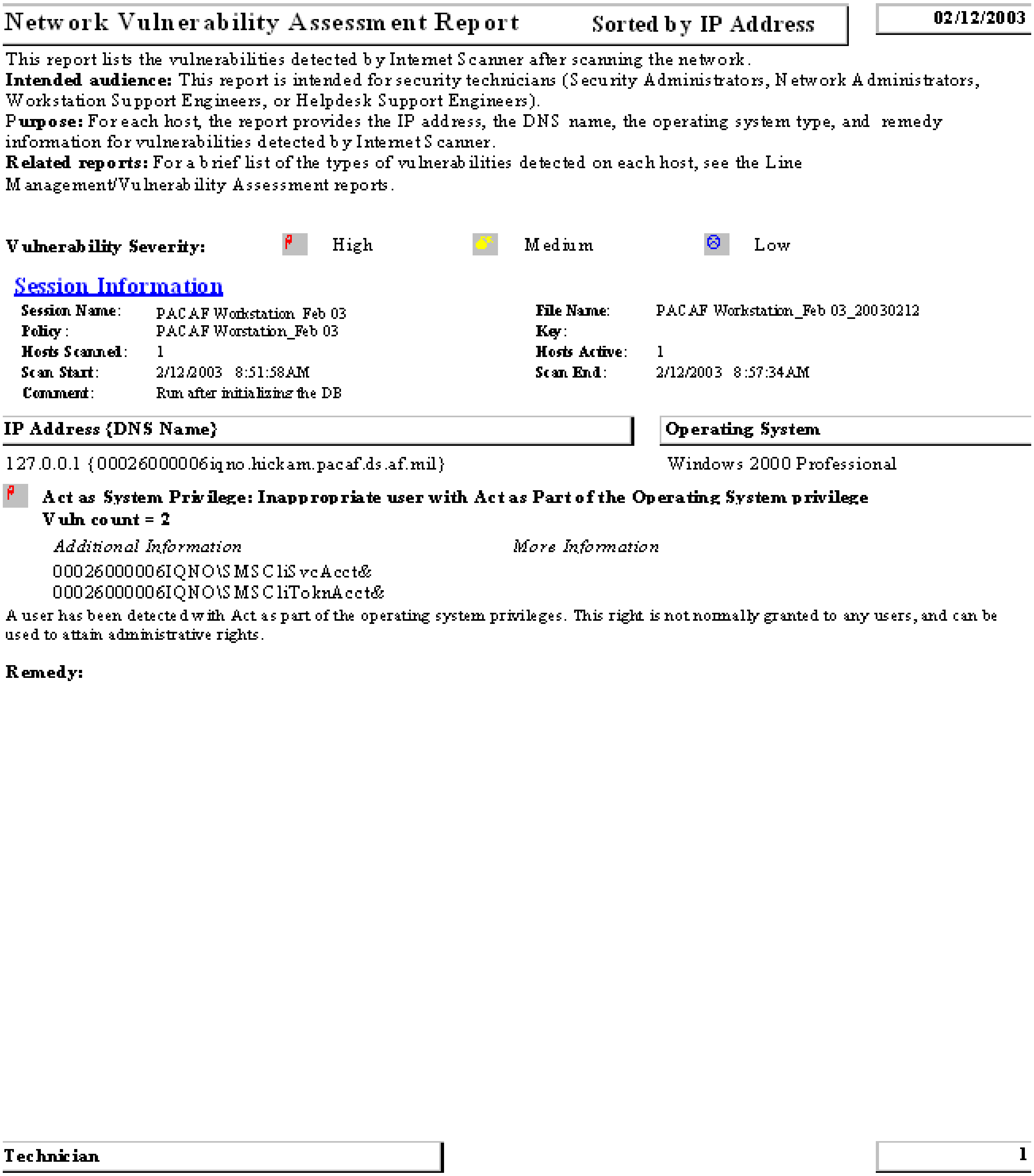
A registry key that can lead to higher access levels is writable by non-administrators. Each of these keys can be used to insert a Trojan horse program that is then invoked when another user logs in. The AeDebug key can be used to directly gain higher access if the attacker can cause a service running at a privileged user level to crash.

The vulnerable keys under HKEY_LOCAL_MACHINE are:
- Software\Microsoft\Windows\CurrentVersion\Run
- Software\Microsoft\Windows\CurrentVersion\RunOnce
- Software\Microsoft\Windows\CurrentVersion\RunOnceEx
- Software\Microsoft\Windows NT\CurrentVersion\AeDebug
- Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options

Line Management | **1**

Attachment 13 (Added)

SAMPLE TECHNICIAN VULNERABILITY ASSESSMENT REPORT



Network Vulnerability Assessment Report Sorted by IP Address **02/12/2003**

This report lists the vulnerabilities detected by Internet Scanner after scanning the network.
Intended audience: This report is intended for security technicians (Security Administrators, Network Administrators, Workstation Support Engineers, or Helpdesk Support Engineers).
Purpose: For each host, the report provides the IP address, the DNS name, the operating system type, and remedy information for vulnerabilities detected by Internet Scanner.
Related reports: For a brief list of the types of vulnerabilities detected on each host, see the Line Management/Vulnerability Assessment reports.

Vulnerability Severity: 🟥 High 🟨 Medium 🟦 Low

Session Information

Session Name:	PACAF Workstation Feb 03	**File Name:**	PACAF Workstation_Feb 03_20030212
Policy:	PACAF Worstation_Feb 03	**Key:**	
Hosts Scanned:	1	**Hosts Active:**	1
Scan Start:	2/12/2003 8:51:58AM	**Scan End:**	2/12/2003 8:57:34AM
Comment:	Run after initializing the DB		

IP Address {DNS Name}	**Operating System**
127.0.0.1 {00026000006iqno.hickam.pacaf.ds.af.mil}	Windows 2000 Professional

🟥 **Act as System Privilege: Inappropriate user with Act as Part of the Operating System privilege**
Vuln count = 2

Additional Information	*More Information*
00026000006IQNO\SMSCliSvcAcct& 00026000006IQNO\SMSCliToknAcct&	

A user has been detected with Act as part of the operating system privileges. This right is not normally granted to any users, and can be used to attain administrative rights.

Remedy:

Technician 1

Attachment 14 (Added)

IC 2003-1 TO AFSSI 5021/PACAFSUP1, TIME COMPLIANCE NETWORK ORDER (TCNO) MANAGEMENT AND VULNERABILITY AND INCIDENT REPORTING

25 JULY 2003

SUMMARY OF REVISIONS

This change adds procedures and CONOPS to the PACAF wireless network scanning initiative. This change sets forth operating and reporting procedures for wireless networks and devices found on the PACAF Enterprise. A bar (|) indicates revision from previous edition.

3.1.2. (Added). Internet Security Systems Wireless Scanner is PACAF's wireless network scanning tool of choice and is fielded to all PACAF bases as an enhancement to the approved CITS NMS/BIP toolset. As such, all PACAF bases must use Wireless Scanner to perform wireless network vulnerability scans. Each base has at least one individual who is Internet Scanner certified. His/her duties will encompass ISS Wireless Scanner. This Internet Scanner "certified" individual can train others in the crew position but he/she cannot certify them.

3.1.2.1. (Added). Ministumbler is a used to pinpoint wireless networks while walking through buildings. It will not test for vulnerabilities but will aid in the location of wireless devices on PACAF installations.

3.5.1.13. (Added). Wireless Scans. Each base will conduct wireless network scans on a periodic basis. This scan will be tasked by a Time Compliance Technical Order (TCTO) on a periodic basis. Upon discovery of a wireless network the ISS technician needs to verify its validity. This is done by verifying a signed AF Form 3215, and a Certificate to Operate from the DAA.

3.5.1.13.1. (Added). If a wireless network is found and is not authorized, a solution for the customer must be presented before any equipment is confiscated.

RONNIE D. HAWKINS, JR., Colonel, USAF
Director, Communications and Information